Exhibit M

RIDGEVIEW MEDICAL CENTER AND CLINICS **#3521**

SUBJECT: VENDOR/THIRD-PARTY ACCESS POLICY

ORIGINATING DEPT: Information Technology (IT) **DISTRIBUTION DEPTS:** All

ACCREDITATION/REGULATORY STANDARDS:

Original Date: 12/12 **Revision Dates:** **Reviewed Dates:**	**APPROVAL:** Administration: _____ Director: _____

PURPOSE:

The purpose of the Ridgeview Medical Center Vendor Access Policy is to establish the rules for vendor access to Ridgeview Medical Center Information Resources and support services (A/C, UPS, PDU, fire suppression, etc.), vendor responsibilities, and protection of Ridgeview Medical Center information. Vendor access to Ridgeview Medical Center Information Resources is granted solely for the work contracted and for no other purposes.

Audience

The Ridgeview Medical Center Vendor Access Policy applies to all individuals that are responsible for the installation of new Ridgeview Medical Center Information Resource assets, and the operations and maintenance of existing Ridgeview Medical Center Information Resources, and who do or may allow vendor access for support, maintenance, monitoring and/or troubleshooting purposes.

POLICY:

- Vendors must comply with all applicable Ridgeview Medical Center policies, practice standards and agreements, including, but not limited to:
  - Safety Policies
  - Privacy Policies
  - Security Policies
  - Auditing Policies
  - Software Licensing Policies
  - Acceptable Use Policies
- Vendor agreements and contracts must specify:
  - The Ridgeview Medical Center information the vendor should have access to
  - How Ridgeview Medical Center information is to be protected by the vendor
  - Acceptable methods for the return, destruction or disposal of Ridgeview Medical Center information in the vendor's possession at the end of the contract
  - The Vendor must only use Ridgeview Medical Center information and Information Resources for the purpose of the business agreement
  - Any other Ridgeview Medical Center information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others
- Ridgeview Medical Center IS will provide a technical point of contact for the vendor. The point of contact will work with the vendor to make certain the vendor is in compliance with these policies.

- Each vendor must provide Ridgeview Medical Center with a list of all employees working on the contract. The list must be updated and provided to Ridgeview Medical Center within 24 hours of staff changes, wherever possible.
- Each vendor employee with access to Ridgeview Medical Center Confidential Data must be approved to handle that information at a level commensurate with its classification level.
- Vendor personnel must report all security incidents directly to the appropriate Ridgeview Medical Center IS personnel.
- If vendor management is involved in Ridgeview Medical Center security incident management, the responsibilities and details must be specified in the contract.
- Vendor must follow all applicable Ridgeview Medical Center change control processes and procedures.
- If appropriate, regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate Ridgeview Medical Center IS Management.
- All vendor maintenance equipment on the Ridgeview Medical Center network that connects to the outside world via the network, telephone line, or leased line, and all Ridgeview Medical Center Information Resource vendor accounts will remain disabled except when in use for authorized maintenance.
- Vendor access must be uniquely identifiable and password management must comply with the Ridgeview Medical Center Policy #3516 – *Passwords* and Policy #3503 – *Administrator/Special Access.*
- Vendor's major work activities must be entered into a log and available to Ridgeview Medical Center IS Management upon request. Logs must include, but are not limited to, such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times, wherever possible.
- Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to Ridgeview Medical Center or destroyed within 24 hours.
- Upon termination of contract or at the request of Ridgeview Medical Center, the vendor will return or destroy all Ridgeview Medical Center information and provide written certification of that return or destruction within 24 hours.
- Upon termination of contract or at the request of Ridgeview Medical Center, the vendor must immediately surrender all Ridgeview Medical Center badges, access cards, equipment and supplies. Equipment and/or supplies to be retained by the vendor must be documented by authorized Ridgeview Medical Center IS Management.
- Vendors are required to comply with all regulatory and Ridgeview Medical Center auditing requirements, including the auditing of the vendor's work.
- All software used by the vendor in providing service to Ridgeview Medical Center must be properly inventoried and licensed.
- Each vendor granted access to any Ridgeview Medical Center Information Resource must sign the Ridgeview Medical Center Information Security Policy Acknowledgement Form which stipulates that he/she:
    - Has read and understands the security policies.
    - Understands his/her responsibilities to comply.
    - Understands the consequences of an infraction.

WAIVERS:
Waivers from certain policy provisions may be sought following the process outlined in the Ridgeview Medical Center Policy #3511 – *Enterprise Information Security Governance.*

ENFORCEMENT:
Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights and termination of contract(s).

VERSION HISTORY OF SOURCE DOCUMENT: Ridgeview Medical Center Information Security Policy Manual

Version Number	Date	Reason/Comments
V1.00	December, 2012	Document Origination
V2.00	May, 2014	Full review with IT Steering Committee
V3.00	August, 2015	Reviewed with Security Committee
	6/16	Finalized, assigned policy number, on RidgeNet. Previous documentation not archived.